ISMG Draft Meeting Minutes

Date: March 31, 2011

Time: 1:00 pm

Location: Walt Sullivan Building, First Floor conference room

Attendees

Pat Boles, SITSD; Bill Hallinan, TRS; Cleo Anderson, REV; David Swenson, MPERA; Chris Silvonen, DPHHS; Barney Benkelman, FWP; Larry Krause, COM; Rick Bush, DNRC; and Monica Abbott, SITSD.

Call to Order – Pat Boles

- Pat Boles called the March meeting to order and asked everyone to introduce themselves.

Approval of Minutes – Pat Boles

- Pat asked for comments or changes to the February minutes. Rick mentioned the name of ISMG was not listed on the minutes. Pat will make the change.
  **** Action Item****
- Barney Benkelman offered a motion to approve the corrected minutes. Rick Bush seconded.
    - Motion passed unanimously.

Discuss Affinity Theme Summary Document – Pat Boles

- Pat reported the document is a summary of the themes noted on the post-it notes collected during the February meeting. Pat asked for everyone to review to ensure all data was captured. This will allow ISMG to plan how best to move forward.
- Barney commented about the need to simplify the complexity of NIST security information in order to explain the requirements to top management. Pat replied that the newly published NIST 800-39 addresses the compliance issues in order to customize the controls that need to be put into place. Bill Hallinan mentioned that his director only wants to see a top level document. He suggested a summary document showing the policy, the security plan, the state framework controls, the application categorization, and the controls going with that.
- Rick Bush offered that information needs to be shown differently for various organizational levels to get the information that each level needs. List what are the state statutes that apply. Cleo Anderson added to identify requirements. Consequences can be a huge negative for agencies.
- Pat mentioned the NIST 800-39 is the first step in managing controls.
- Larry Krause added that we go down different roads and often make little progress. Rick offered to not put in a control until there is a need for the control.
- Cleo mentioned in their federal audit, not having written documentation in place was the violation mentioned most often.
- Barney commented that Cleo's audit example shows to look at NIST and see what we really need to focus on. Cleo mentioned that Lynne Pizzini works on this already.

- Bill mentioned that it would be good to have a standard at the state level that would include training.
- Simplify the policy, implement the procedure.
- Rick offered an edit in the second paragraph to simplify the sentence to read "Have an open forum for discussion with their peers".

Discuss ISMG Rules of Procedure – Pat Boles

- Pat noticed there was previous discussion about rules of procedure. Pat asked for changes from the group.
- Rick asked to add designee in the overview in reference to the membership. Designated representative listed as part of the membership and participation. The Chair will remain to be the EISB bureau chief. There is a redundancy of member participation which will be removed.
- The group discussed whether or not the Agency Director would be contacted if attendance slipped and the team recommended that he/she would not be called if there is no participation. Bill asked about if the group recommends something without having participating agencies.
- Rick offered to remove notification and leave continuity and consistency. Rick asked about minutes being needed. Cleo mentioned it is good to have a record especially if members are unable to attend.
- The changes will be made and the document will be at the next meeting for approval.
- Chris Silvonen mentioned that there is a concern on the representing the agency by voting, which may not be in alignment with the Agency Director.
- Larry and Barney both mentioned this group is just offering recommendations.
- Pat will review Project Management Office Advisory Group (PMOAG) Rules of Procedure and use the language found there on voting.
- Barney asked about Thursdays and not Tuesdays as listed. Pat will make all pertinent changes.

Discuss NIST 800-39 Managing Information Security Risk – Organization, Mission, and Information System View – Published March 2011

NOTE: Policy-20090701a Statewide Information Security Policy Information Security Programs point in the policy statement to ***DRAFT*** **NIST SP 800-39 Managing Risk from Information System** first published three years ago. The document was published as a ***FINAL*** document in the last month; the title is now **NIST SP800-39 Managing Information Security Risk – Organization, Mission, and Information System View**.

- Pat spoke about managing risks using NIST 800-39 and what he thinks will clarify what is due by 2012. He shared the handout below to clarify his points. http://ent.sharepoint.mt.gov/groups/ism/Shared%20Documents/Meeting%20Documents/2011%20_03_March/Info_Risk_Mgmt_2011_03.pdf. Since this is a shift, there will be more discussions in the future on the impact that this updated NIST 800-39 will have in implementation of the policy.
- There is a hierarchy of documents within the Information Risk Management Policy of which NIST 800-39 is a standard that sets the foundation.

- There are three tiers of risk management activities and processes with agency (organizational) level as the top tier, mission and business process as the second tier and the actual information systems as the third tier. The organizational or agency perspective will define the risk frame, it sets the foundation for the risk management program. The next layer will show how the mission and business process will utilize information security to meet the requirements. The lowest level is the operational technical controls in the informational world.
- The life cycle of the risk management strategy approach gives determination of risks, information generation, and implementation of selected courses of action.
- The enterprise review process is utilizing the life cycle with PMO requirements. Pat suggested there may be reports in the future from the group to be used as a center of excellence. The goal is to provide relevant and accurate information for the decision making stakeholder processes. Tweak and modify until it meets our needs through our business requirements.
- The "Framing" of risk outlines a process to identify the risks. Using inputs and activities, the output will produce a risk management strategy document and other documents including organizational policies, standards, guidelines and resources.
- Pat is looking for templates for the Risk Management Strategy, but has not found any yet.
- "Assessing" risk looks at inputs and activities from "Frame", "Respond," and "Monitor Risk", this sets the framework for a continuous monitoring and improvement process.
- By 2012, the thought at this time is to focus on developing individual agency initial Risk Management Strategy Document, then identify the agencies' systems and assess the risks to those systems. Finally, taking the output from the "Assess" risk process, each agency will update their Risk Management Strategy Document.
- Pat would like to see if this approach would be approved by the consensus of the group after the documents are reviewed.
- In the "Responding to Risk" process, the inputs from the "Frame" and "Assess" process outputs lead to an implementation of selected courses of action.
- "Monitoring" process takes input from the other risk processes. Outputs verify that required risk response measures are implemented, determine ongoing effectiveness, and identify changes to information systems, and environments of operation (i.e. new or modified requirements, legal mandates, etc). In short, the output is information generated that leads back to frame risk, respond to risk and assess risk.
- Pat would like the group to review NIST 800-39 and have a more in depth discussion at the next meeting.

Update – Where we are at, charter, and policies – Pat Boles

- The charter is not a required document from this group
- Pat asked about policy documents to work on in the future. He has the Standards for the Security Access Control and Identification and Authentication and asked if the group still wants to work on the documents.
- Cleo suggested the group review the documents before the next meeting.
- Pat will make changes suggested by legal and send these out to the group within 2 weeks.

- Bill mentioned he understood that we are to have one operating standard document.
- Cleo added that eventually the state policies would be followed unless each agency has a unique need. Barney mentioned policies would depend where the service is located. Larry added the agencies would set the rules for each agency.
- Bill asked if the security program is enough based on NIST then where do the policies come in. Larry asked if the policies are going away in 2012. Pat will find that out.
- Pat stated the right direction of a policy is to be an enabler. Policies will state what you can do within constraints. Every agency has different needs but may need a common set of controls.
- In further discussion on this topic, the Federal "Cloud First Policy," was discussed. The policy requires federal agencies to find three systems to move to the cloud and to plan for them. The first system is to be fully implemented in the cloud within 12 months, the second two within 18 months. The issue from the Federal perspective was using the cloud services, while still meeting compliance requirements. The DRAFT FedRAMP program has a set of NIST controls for low and moderate category systems. The service provider certifies that the requirements are met, and validates through reporting back to the federal agencies their implementation / monitoring of the security requirements. Maybe this is something that we can use in the future.
- The Internet and Intranet Security and Internet Filtering Standards that were to be rescinded are not in a decision brief. Pat is still trying to figure out where these documents fit. The documents have been received back from Step 5 in the Development Phase of the IT Policy and Standard Development Procedure.
- Pat will bring those documents to the meeting next month.

EPA ASSERT - Bill Hallinan

- Bill gave a presentation of his security documents.
- He showed his security plan which was developed from NIST and talked about how he manages the plan with checklists. Bill has a security plan, the security assessment report and the plan of actions and milestones – three deliverables for his agency.
- He found that EPA has developed a system called ASSERT that could be used across all of our state agencies. He contacted EPA and they sent Bill their source code and database.
- This tool talks about organization, systems, assessments, reports and databases, and administration. It can be used by the three branches of state government and agencies added to each branch. It allows you to add bureaus and sections to be as detailed as needed. Systems can be added to allow a price to be given to it. Categorizing allows more information to be added along with supplemental guidance.
- All of the detailed work of the tool results in a report.
- Larry asked about the group being able to check it out. Bill will check to see if he can add everyone so they can look at the site.
- Larry asked if it is mainly for the security manager for monitoring. Bill replied it can be used with your control people by implementing a control and it shows why. The testing component allows you to test the implementations. Cleo suggested putting policies into the informational area. Hyperlinks can be put into the areas.

- Bill showed his dashboard when he logged into the system. There are built-in milestones. It appears to have an auditing component.
- Pat will add Bill to the agenda for next month.

Other Business or Concerns – ISMG

- Pat mentioned there is online video awareness training available from MS-ISAC. Securing the security awareness with 19 modules with a charge of $1.15 per seat. If MS-ISAC does not fill enough seats, the price will increase to around $1.40 per seat. It is not known if this charge is per module or all 19 modules together. To take advantage of this opportunity, commitment is needed by April 30th and payment must be made by June 30. Larry asked about previewing. Pat will put a PowerPoint presentation out on the SharePoint site. If you are interested in participating, please send an email to Lynne Pizzini and CC Jere Hoy with how many seats you will purchase.
- Cleo asked about social networking. Larry uses a two page form to be filled out by the requesting individual. It is reviewed the application by legal. Cleo asked about concerns of confidential information. Larry will send form he developed to Cleo.
- Chris mentioned that many systems can be listed as moderate according to the standards in NIST.

Adjourn – Pat Boles

- The meeting adjourned at 2:44 pm.